

**America's Health
Insurance Plans**

601 Pennsylvania Avenue, NW
South Building
Suite Five Hundred
Washington, DC 20004

202.778.3200
www.ahip.org



October 16, 2007

SENT VIA EMAIL TO kcohen@ftc.gov
Federal Trade Commission
Division of Privacy and Identity Protection
Attention: Kristin Krause Cohen
600 Pennsylvania Avenue, N.W.
Washington, D.C. 20580

Re: Your Request for Information Relating to Uses of Social Security Numbers by Health Insurance Plans

Dear Ms. Krause Cohen:

America's Health Insurance Plans (AHIP) is the national association representing nearly 1,300 health insurance plans providing coverage to more than 200 million Americans. Our members offer a broad range of products in the commercial marketplace including health, long-term care, dental, vision, disability, and supplemental coverage. Our members also have a strong track record of participation in Medicare, Medicaid, and other public programs.

AHIP is writing to offer general comments in response to your request for information relating to uses of Social Security Numbers (SSNs) by health insurance plans. We understand that the FTC is compiling information about the private industry's uses of SSNs for the President's Identity Theft Task Force to evaluate practical ways to curb the occurrence of identity theft. Your agency has contacted us to provide general information about health insurance plans' uses of SSNs. In response to your request, we have included our general comments in Attachment A.

In addition, health insurance plans are governed by a complex framework of federal and state legal requirements that set strict rules for use, disclosure, and transfers of individually identifiable health information. We have compiled an overview of these requirements in Attachment B.

We stand ready to assist you with other general information that you may require. Should you need additional clarification about these issues, please contact me at (202) 861-1473.

Sincerely,

Marilyn Zigmund Luke
Senior Regulatory Counsel

America's Health Insurance Plans

Attachment A Specific Comments Addressing Health Insurance Plans' Uses of Social Security Numbers October 16, 2007

The following comments are offered about uses of Social Security Numbers (SSNs) by health insurance plans. The subject areas correspond with the public solicitation for comments that was posted on the Federal Trade Commission website at:

<http://www.ftc.gov/opa/2007/07/ssncomments.shtm>.

Current Private Sector Collection and Uses of SSNs

SSNs are used by health insurance plans for purposes related to the proper administration of health plans and policies. We believe that health insurance plans currently have sufficient, stringent protections in place to protect individual consumers' individually identifiable health information, which includes protecting the confidentiality of individuals' SSNs. Subject to federal and state legal requirements, health insurance plans are required to collect or use SSNs for a number of legitimate purposes that include:

- verifying eligibility for governmental health benefits programs. For example, when a private health insurance plan acts as a contractor for the Medicare Advantage or Medicaid programs, SSNs are required to be shared between the governmental agency and the private contractor to verify an individual's eligibility for program participation, eligibility for dual public programs, and for specific payment reconciliation processes. In some situations, state Medicaid plans and their contracted health insurance plans also use SSNs to identify individuals eligible for or receiving health benefits.
- complying with requirements that specify the use of SSNs to execute complete electronic health care transactions.
- tracking payments to health care providers and documenting such for tax reporting purposes (e.g., the Internal Revenue Service 1099 reporting).
- complying with state laws and regulations that require SSNs on standardized insurance forms reviewed, approved, or mandated by the state Insurance Departments. For example, the state of New Jersey requires health insurance plans to collect SSNs on standardized forms (e.g., the standardized application form) approved for use in the individual and small employer health benefits markets.

Other legitimate health insurance plan purposes that can require the collection and use of SSNs include:

- coordinating benefits between private health insurance plans. Often, an individual may have health coverage through an employer plan and maintain concurrent

health coverage under a spouse's employer health plan. When more than one health plan or policy is available for an individual, private health insurance plans need to coordinate benefits to ensure that claims are not overpaid.

- coordinating benefits between public and private sector entities. For example, most group and individual long-term disability carriers reduce the amount of private disability income benefits by the amount of Social Security Disability Insurance (SSDI) benefits. Such coordination of private and public disability income benefits helps to ensure that the income of an individual who is receiving disability income benefits from more than a single source does not have disability income that approaches or exceeds pre-disability income.
- establishing administrative process which allows a health insurance plan to follow the federal Medicare Secondary Payer (MSP) law and regulations on an employer's behalf.¹ Generally, the MSP requirements enumerate whether the employer plan should be processing claims as a primary or secondary payer before submitting claims to the Medicare program for payment.²
- establishing administrative processes to enable compliance with the Deficit Reduction Act of 2005.³ This Act expanded the ability of state Medicaid plans to pursue third parties (e.g., health insurance issuers, employer group health plans) for reimbursement of funds.
- using an individual's SSN to help accurately identify an individual for participation in disease management activities, public health reporting, and quality assurance reviews.
- receiving SSNs from employers who rely on SSNs as the primary identifier to accurately enroll and disenroll employees and their eligible dependents.
- using SSNs when coordinating treatment and care with the provider community. Historically, within the overall health care community the SSN is the one identifier that has been consistently used to track an individual's health encounters over his or her lifetime. SSNs can be used to access individuals' historical and archival information within electronic databases for this purpose.
- transferring business records containing SSNs that identify customers and providers during business mergers or acquisitions.
- allowing individuals who want the ability to use their own SSN as a convenience to identify themselves to their health insurance plan instead of using a health plan assigned identifier from an identification card.

Currently, most private health insurance plans are moving away from using or displaying SSNs relating to members, customers, or contracted health care providers on identification cards, correspondence, as well as checks and related documentation. In

¹ The MSP provisions mandate coordination of benefits between employer group health plans and the Medicare program (42 U.S.C. §1395y *et seq.* and 42 C.F.R. Part 411).

² Group health plans are subject to the MSP provisions. Generally, if an individual is covered by the plan and Medicare and the plan is established by or receives contributions from an employer that has "20 or more employees for each working day in each of 20 or more calendar weeks in the current calendar year or the preceding calendar year," then the group plan is responsible for processing claims as a primary payer before submitting claims to the Medicare program for payment. (42 U.S.C. §1395y (b)(1)(A)(ii, iii).

³ Refer to 42 U.S.C. §1396a(a)(25).

some cases, health insurance plans have truncated SSNs to limit the amount of information that may be used or viewed for a particular purpose. Further, in some cases, state law requirements (discussed in more detail in Attachment B) prompted such changes, but these changes have also been implemented at the request of business customers such as employers, contracted health care providers, or individual consumers.⁴

The Role of the SSN as an Authenticator

As mentioned above, the SSN has been effectively used within the health care system by providers, health insurance plans, and governmental health benefits programs as a way to accurately identify individuals. Employers may also use SSNs to verify enrollment in a health benefits plan and to accurately track and record certain transactions related to tax reporting.

In the U.S. healthcare system, there has been reluctance to establish a national individual identifier as an alternative to using SSNs, despite a federal statutory requirement under the Health Insurance Portability and Accountability Act (HIPAA) for the U.S. Department of Health and Human Services (HHS) to establish such a system. This issue has been debated for many years and has proven to be quite controversial for a variety of reasons, including privacy concerns. To date, HHS has declined to issue any national individual identifier requirements. Absent this, SSNs have been relied on and continue to be an effective method for identifying individuals for purposes related to their health care.

The SSN as an Internal Identifier

As discussed above, most health insurance plans are moving away from using the SSN as a public, external identifier. However, there are a number of legitimate business needs that require SSNs to be used internally by health insurance plans.

The downside of using internally developed identifiers is that once the new identifier is developed, it is “company specific” – meaning that it will likely not be remembered or used to track an individual who changes health care providers, health insurance plans, employers, and so on. With the federal initiatives to move toward a national, electronic health information exchange, the lack of a single system and method to accurately identify individuals can make accomplishing an effective system quite challenging and can severely inhibit consumers from having a complete medical history over the course of their lives. Some of the potential consequences of using company specific numbers

⁴ The Government Accountability Office (formerly the General Accounting Office) issued a report in January 2004 which provides an overview of the collection and uses of SSNs in the private sector. The report is entitled, “Social Security Numbers: Private Sector Entities Routinely Obtain and Use SSNs, and Laws Limit the Disclosure of This Information. The report is available at: <http://www.gao.gov/new.items/d04111.pdf>.

rather than SSNs could be that individuals' medical histories and records become incomplete, electronic health information eventually is stored in "information silos" because private entities and governmental agencies have an inability to verify individuals and share and transfer information, and eligibility for public or private health benefits may be disputed or not accurately recorded.

The Role of the SSN in Fraud Prevention and Identity Theft

Health insurance plans are accustomed to reviewing and investigating instances of suspected medical coverage fraud or abuse. Most health insurance plans have developed anti-fraud programs that can include establishing special investigational units and devoting substantial resources for anti-fraud initiatives.

Health insurance plans aggressively pursue fraud or over-billing by providers and individuals and seek to obtain monetary recoveries because of statutory or contractual requirements to pay only legitimate, medically necessary claims. Such activities also act as a deterrent for future unlawful activity. Many health insurance plans have built strong relationships with federal and state law enforcement personnel to facilitate reporting and investigation of such situations.

Within the healthcare arena, anecdotal information indicates that traditional identity theft⁵ using an individual's health insurance identifier is rare. However, medical coverage theft⁶ has been prevalent within the industry for many years.

SSNs can be helpful in identifying situations where potential medical coverage fraud or theft has occurred. For example, in some situations, individuals may fraudulently use a false or stolen SSN unbeknownst to an employer to gain employment and thus receive health insurance benefits offered by the employer. In some situations, an employer may be aware that an individual is using a false SSN but allows the improper use to enable the individual to enroll in the employer's health insurance plan. In these situations, the SSN can be a reliable indicator of potentially fraudulent situations and can help a health insurance plan detect and investigate improper situations.

While health insurance plans are using best efforts to combat fraud, new techniques used by unscrupulous individuals can make identifying these improper situations quite challenging. We would support recommendations or advice from the Identity Theft Task Force that promotes better methods for private sector entities to prevent or detect any type of identity theft and we encourage the Task Force's support for using SSNs to combat such illegal activities.

⁵ In this context, traditional identity theft is intended to broadly describe situations where an individual's personal information is accessed or stolen and then used for unlawful purposes, such as fraudulently obtaining a line of credit.

⁶ In this context, medical coverage theft is intended to broadly describe situations where someone uses an individual's medical identification card to access care by posing as the individual or by submitting claims for services that were not legitimate or rendered.

Conclusion

In summary, health insurance plans have and will continue to invest resources to implement safeguards to assure and maintain the confidentiality of their consumers' individually identifiable information. If a specific company collects and uses SSNs for health care operations, that information would be subject to such protections. We encourage the FTC to carefully evaluate the legitimate uses and existing protections for SSNs in the private sector. We hope that the information above adequately explains the current protections for SSNs, and how health insurance plans may serve as a model for other areas within the private sector that do not have similar protections in place.

Attachment B
Overview of Federal and State Laws and Regulations
October 16, 2007

HIPAA

Health insurance plans are governed by a complex framework of federal and state legal requirements. At the federal level, the Health Insurance Portability and Accountability Act of 1996 (HIPAA) sets comprehensive requirements for health insurance plans.⁷ Specifically, Title II of HIPAA established “administrative simplification” standards⁸ for health information privacy, security, identifiers, and for electronic transactions and data elements.

The U.S. Department of Health and Human Services (HHS) later released a comprehensive series of regulations to carry out the HIPAA administrative simplification provisions. The HIPAA Privacy Rule (45 CFR Parts 160 and 164) governs the use and disclosure of individually identifiable health information by health plans and insurers, health care providers, and health care clearinghouses. The HIPAA Security Rule (45 CFR Parts 160, 162, and 164) established standards for protecting data transmission and storage of health information. Therefore, if a health insurance plan collects and uses SSNs of their members or insureds, the SSNs would be protected by the HIPAA requirements.

GLBA

The Gramm-Leach-Bliley Act (GLBA) was passed in 1999 to modernize the financial services industry. Although the legislation was primarily intended to permit “financial institutions” (banks, insurance companies, brokerage houses, and related businesses) to merge and undertake new business activities, a number of GLBA provisions address the disclosure of “non-public personal information.” Generally, health insurance plans must comply with the GLBA requirements which can include providing a notice of privacy practices to its customers and consumers, and allowing individuals the opportunity to “opt-out” of having their information shared with third parties. Under the GLBA, if a health insurance company collects SSNs, that information and any other non-public personal information would be governed by the GLBA requirements.

⁷ If a health insurance plan contracts with a business associate (i.e., a vendor) to help administer health insurance coverage, the business associate is required by contract to adhere to the privacy and security protections. HIPAA sets strict contractual requirements for health insurance plans that use business associates to act on their behalf. For more information, refer to 45 C.F.R. §§ 164.314(a) and 164.504(e).

⁸ The HIPAA administrative simplification provisions apply to group health and individual health plans and policies as well as employer-sponsored plans established under the Employee Retirement Income Security Act. See 42 U.S.C. §1320d for more information.

State Requirements

In addition to the federal requirements, health insurance plans are subject to a wide variety of state laws regulating the use or disclosure of health information. For example, many states require private sector entities to notify consumers in the event that their personal information is included in a data breach (e.g., such as when a hacker unlawfully penetrates a computer database). In addition, most states now prohibit the public display of SSNs on mailings, certain documents such as checks, and on individual health insurance identification cards.